What is claimed is:

1. A method of managing a network session comprising:

delivering policies from a server to a remote system that has predetermined configuration information;

establishing a secure connection between the server and the system; and

regulating activities in the system based on at least one of the set of policies and the predetermined configuration information.

2. The method of claim 1 wherein regulating the activities comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria.

3. The method of claim 2 wherein the rejection criteria include the predetermined static configuration information.

4. The method of claim 2 wherein the rejection criteria include the set of policies.

5. The method of claim 1 wherein regulating the activities comprises providing a session layer adapted to reject unauthorized data packets based on context such as user and application information.

6. The method of claim 1 wherein regulating the activities comprises:

providing a session layer adapted to reject unauthorized data packets based on context information; and

providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies.

7. The method of claim 1 further comprising updating the set of policies.

8. The method of claim 1 further comprising:

detecting data packets from the regulated activities; and

rejecting the data packets from the regulated activities.

9. An article comprising a computer-readable medium which stores computer-executable instructions for managing a network session, the instructions causing a computer to:

receive a set of policies from a server in a remote system having predetermined configuration information;

establish a secure connection between the server and the system; and

manage activities in the system based on at least one of the set of policies and the predetermined configuration information.

10. The article of claim 9, further comprising updating the set of policies.

11. The article of claim 9 wherein the instructions to reject the intervening processes comprises instructions to provide filters that are adapted to reject data packets based on rejection criteria.

12. The article of claim 11 wherein the rejection criteria includes predetermined static configuration information.

13. The article of claim 11 wherein the rejection criteria includes the set of policies.

14. The article of claim 9 wherein the instructions to reject the unauthorized activities comprises instructions to provide a session layer adapted to reject unauthorized data packets based on context user and application information.

15. The article of claim 9 wherein the instructions to reject the unauthorized activities comprises instructions to:

provide a session layer adapted to reject unauthorized data packets based on context information; and

provide filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies.

16. The article of claim 9, further comprising instructions to:

detect unauthorized data packets from the unauthorized activities; and

reject the unauthorized data packets from the unauthorized activities.

17. A network system, comprising:

first and second devices, wherein the first device is adapted to:

deliver a set of policies to the second device;

and the second device is adapted to:

detect data packets from unauthorized activities; and

reject the data packets from the unauthorized activities.

18. The system of claim 17 further comprising a network stack.

19. The system of claim 18, wherein the network stack comprises:

a policy engine connected to the first device;

a policy store connected to the policy engine;

a socket interceptor connected to the policy engine; and

a packet guard connected to the policy engine.

20. The system of claim 17, the first device further comprising instructions to monitor the system for the intervening processes.

21. A network stack, comprising:

a policy engine;

a policy store adapted to interact with the policy engine and store a set of policies from the policy engine;

a socket interceptor coupled to the policy engine;

a packet guard coupled to the policy engine.

22. The network stack of claim 21 further comprising a packet translator adapted to interact with the socket interceptor and the packet guard.

23. The network stack of claim 21 further comprising an interface to a network adapted to connect the network stack to the network, wherein the network has a policy server.

24. The network stack of claim 23 further comprising a configurable management process adapted to reconfigure the network stack and having instructions to:

receive policies in the policy engine from the policy server;

use the socket interceptor to detect and reject data packets from unauthorized users and applications and provide the packet guard with context information about the unauthorized users and applications;

use the packet guard to filter unauthorized activities received from the network interface;

use the packet guard to filter the data packets from unauthorized users and applications based on the context information received by the socket interceptor; and

use the packet guard to filter data packets based on the policies.